The rapid advancement of technology is causing ripple effects in every area of society, including politics. It seems as though war has received an upgrade. A new style of attack has been added to the arsenal known as cyber warfare, and it is getting political attention around the world. PCWorld posted an article, on June 10, 2012; titled Cyber warfare gets Political[[1]](#footnote--1). The PCWorld post discusses an article released by the *New York Times* stating that President Obama and the United States have been using cyber warfare to target Iran’s nuclear program. The attack came in the form of a Stuxnet worm, first discovered in June 2010, which is one of the most sophisticated viruses ever found. The Stuxnet worm, code named ‘Olympic Games’ by the US, has the ability to cripple a country’s entire infrastructure. Many people fear that the publicity involved with the most recent cyber attack will bring immanent harm upon the United States. Whether or not the Obama administration was really involved with the Stuxnet attack, it has weakened the country’s reputation. The *New York Times* article quotes President Obama expressing concerns that “any American acknowledgement that it was using cyber weapons… could enable other countries, terrorists or hackers to justify their own attacks.” As the recent Stuxnet attack is folded into political agendas and propaganda, it is hard to say who was really behind the attack.

After reading the article summarized above, I did some research on how to defend against the Stuxnet worm. The use of standardized IP technology in control systems underlying a nation’s critical infrastructure has introduced new vulnerabilities, as seen by the recent appearance of the Stuxnet worm. The National Institute of Standards and Technology has published guidelines for defending against attacks such as this in Special Publication 800-82, [Guide to Industrial Control Systems (ICS) Security](http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)[[2]](#footnote-0). The publication provides “guidance on securing ICS, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). It includes an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.” The methods for defending against the Stuxnet worm vary defending on the IP technology being used. However, it is important to know that there are ways to defend against the Stuxnet virus. Therefore, any system vulnerable to the Stuxnet worm should consider putting the proper protocols in place because prevention is an important step in defending against cyber warfare.

1. http://www.pcworld.com/article/257280/cyberwarfare\_gets\_political.html [↑](#footnote-ref--1)
2. http://gcn.com/articles/2011/06/10/nist-industrial-control-ssytems-security.aspx [↑](#footnote-ref-0)